

Резервирование Интернет-каналов без использования BGP.

Наташа Самойленко

Резервирование провайдеров без использования BGP

Для настройки резервирования требуется совмещение нескольких технологий*:

- Статическая маршрутизация
- IP SLA
- Track (Enhanced Object Tracking)
- Local PBR
- NAT
- EEM (Embedded Event Manager)

* В зависимости от того, какая схема работы требуется, могут понадобиться также и другие технологии

Статическая маршрутизация

Статическая маршрутизация

Схема основной/резервный

Маршрут по умолчанию, который ведет на резервного провайдера, должен быть со значением AD, которое хуже основного.

```
ip route 0.0.0.0 0.0.0.0 70.1.1.100      (основной)
ip route 0.0.0.0 0.0.0.0 80.1.1.100 250  (резервный)
```

Балансировка трафика

Оба маршрута по умолчанию должны быть с одинаковым значением AD:

```
ip route 0.0.0.0 0.0.0.0 70.1.1.100
ip route 0.0.0.0 0.0.0.0 80.1.1.100
```

Статическая маршрутизация

Статический маршрут остается в таблице маршрутизации до тех пор, пока маршрутизатор может найти путь к next-hop.

Если проблема находится внутри сети провайдера, или за ее пределами, с помощью обычного статического маршрута её обнаружить нельзя.

РЕШЕНИЕ:

настроить тест для проверки доступности выбранных ресурсов в Интернет (IP SLA) и сделать так, чтобы статический маршрут по умолчанию зависел от результата теста (track).

IP SLA

IP SLA

IP SLA позволяет создавать тесты.

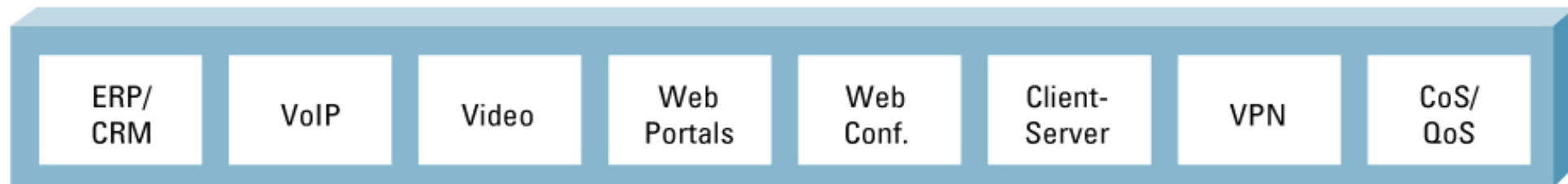
Один из самых простых примеров теста: проверка доступности ресурса с помощью простого “ping” (отправки ICMP-запроса и ожидания ICMP-ответа).

Тесты также могут быть и более сложными. Например, проверка качества канала по таким характеристикам как jitter и delay.

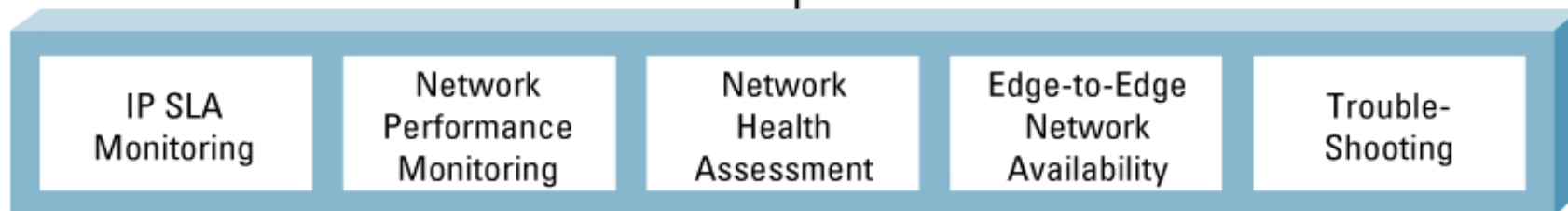
В зависимости от теста, на стороне получателя может быть, или любое устройство с соответствующим сервисом, или оборудование Cisco.

IP SLA, за время существования, сменил несколько вариантов настройки. Поэтому, настройка в другой версии IOS может отличаться от указанной.

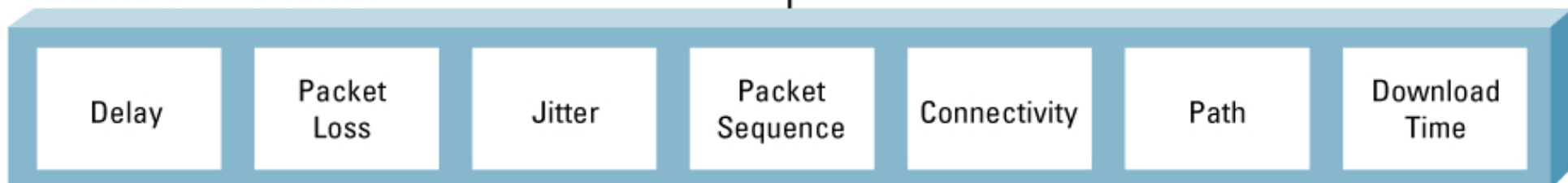
Applications and Solutions



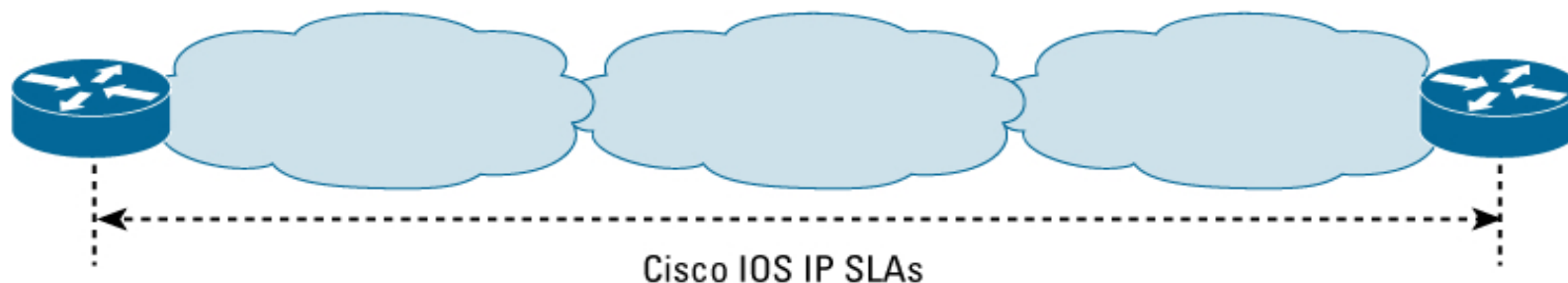
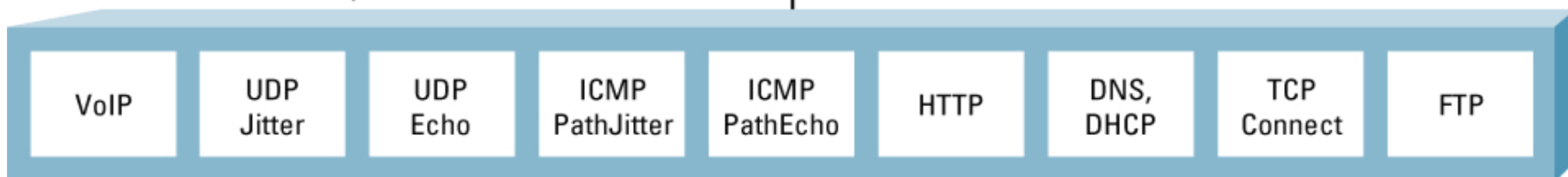
Cisco IOS SLAs Functions



Cisco IOS IP SLAs Metrics



Cisco IOS IP SLAs Operations



Доступные измерения

```
router1(config-ip-sla)#?
```

IP SLAs entry configuration commands:

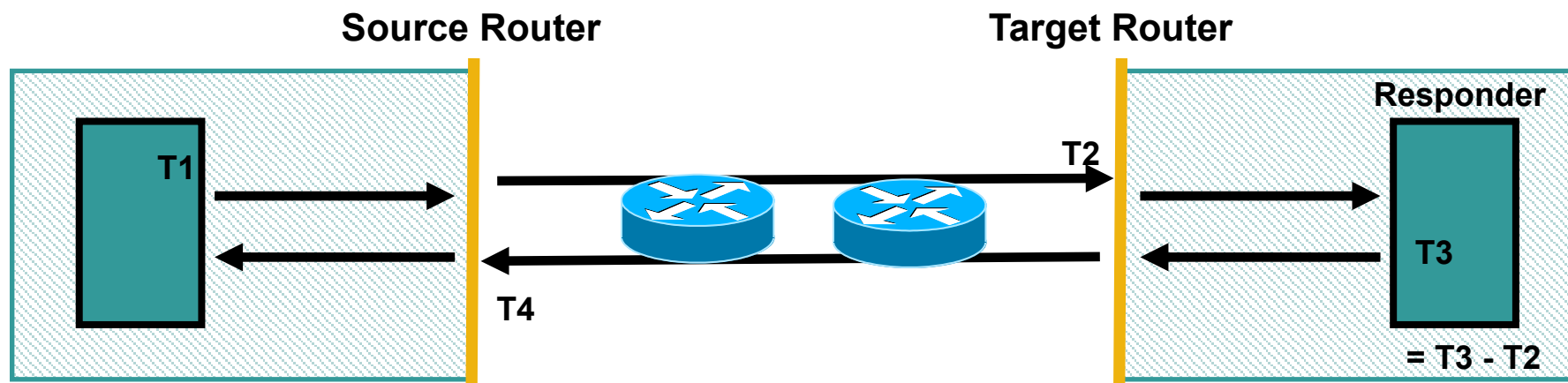
dhcp	DHCP Operation
dns	DNS Query Operation
ethernet	Ethernet Operations
exit	Exit Operation Configuration
ftp	FTP Operation
http	HTTP Operation
icmp-echo	ICMP Echo Operation
icmp-jitter	ICMP Jitter Operation
mpls	MPLS Operation
path-echo	Path Discovered ICMP Echo Operation
path-jitter	Path Discovered ICMP Jitter Operation
tcp-connect	TCP Connect Operation
udp-echo	UDP Echo Operation
udp-jitter	UDP Jitter Operation
voip	Voice Over IP Operation

Пример IP SLA теста (icmp-echo)

```
ip sla 1
  icmp-echo 8.8.8.8 source-interface Gi0/1
  threshold 1000
  timeout 1500
  frequency 3

ip sla schedule 1 life forever start-time now
```

IP SLA Responder



Для ряда тестов, со стороны получателя должно быть оборудование Cisco. Функционал получателя для тестов IP SLA называется ip sla responder.

Responder учитывает время на обработку пакетов маршрутизатором

Responder позволяет выполнять односторонние измерения latency, jitter, packet loss

Пример IP SLA теста (udp-jitter)

Source#

```
ip sla 55
```

```
  udp-jitter 12.13.0.13 16384 num-packets 2000
```

```
  request-data-size 200
```

```
  tos 46
```

```
ip sla schedule 55 life forever start-time now
```

```
ntp server 10.0.0.2
```

Target#

```
ntp server 10.0.0.2
```

```
ip sla responder
```

Проверка настроек

```
router1#sh ip sla summary
```

```
IPSLAs Latest Operation Summary
```

ID	Type	Destination	Stats	Return (ms)	Last Code	Run
*1	icmp-echo	8.8.8.8	RTT=1	OK	1	second ago
*2	icmp-echo	8.8.4.4	RTT=1	OK	2	seconds ago
*3	icmp-echo	4.4.4.4	RTT=1	OK	1	second ago
*55	udp-jitter	12.13.0.13	RTT=1	OK	1	minute, 17 seconds ago

```
router1#sh ip sla statistics
```

```
IPSLAs Latest Operation Statistics
```

```
IPSLA operation id: 1
```

```
Latest RTT: 1 milliseconds
```

```
Latest operation start time: 17:17:34 UTC Tue Feb 17 2015
```

```
Latest operation return code: OK
```

```
Number of successes: 610
```

```
Number of failures: 0
```

```
Operation time to live: Forever
```

Policy-based routing (PBR)

Policy-based Routing (PBR)

Маршрутизация на основе политик (policy based routing, PBR) позволяет маршрутизировать трафик на основании заданных политик, тогда как в обычной маршрутизации, только IP-адрес получателя определяет каким образом будет передан пакет.

Основной объект с помощью которого настраивается PBR: **route-map**

PBR может применяться, как для сквозного трафика, так и для трафика, который генерируется маршрутизатором.

Пример настройки PBR

Настройка PBR для сквозного трафика:

```
ip access-list extended LAN1
  permit ip 10.3.1.0 0.0.0.255 any
ip access-list extended LAN2
  permit ip 10.3.2.0 0.0.0.255 any
```

```
route-map PBR permit 10
  match ip address LAN1
  set ip next-hop 10.0.17.1
route-map PBR permit 20
  match ip address LAN2
  set ip next-hop 10.0.27.2
```

```
interface Ethernet0/1
  ip policy route-map PBR
```


Пример настройки Local PBR

Настройка PBR для трафика, который генерирует маршрутизатор:

```
ip access-list extended SLA_ACL
  permit icmp host 70.1.1.1 host 8.8.8.8
  permit icmp host 70.1.1.1 host 8.8.4.4
  permit icmp host 70.1.1.1 host 4.4.4.4
```

```
route-map PBR_SLA permit 10
  match ip address SLA_ACL
  set ip next-hop 70.1.1.100
```

```
ip local policy route-map PBR_SLA
```

Enhanced Object Tracking (track)

Object Tracking (Enhanced Object Tracking)

Enhanced Object Tracking (track) — это функция оборудования Cisco, которая позволяет отслеживать состояние выбранного объекта и влиять на состояние других функций.

Объекты, состояние которых может отслеживаться:

- Состояние Line-Protocol интерфейса
- Доступность маршрута
- Метрика маршрута
- Состояние IP SLA

Несколько track можно скомбинировать в один

Track и IP SLA

```
ip sla 1
  icmp-echo 8.8.8.8 source-interface Gi0/1
  threshold 1000
  timeout 1500
  frequency 3

ip sla schedule 1 life forever start-time now

track 10 ip sla 1 reachability
  delay down 10 up 5

ip route 0.0.0.0 0.0.0.0 70.1.1.100 track 10
ip route 0.0.0.0 0.0.0.0 80.1.1.100 250
```

Комбинированный track и IP SLA

```
track 10 ip sla 1 reachability
track 20 ip sla 2 reachability
track 30 ip sla 3 reachability
```

```
track 100 list boolean or
  object 10
  object 20
  object 30
  delay down 10 up 5
```

```
ip route 0.0.0.0 0.0.0.0 70.1.1.100 track 100
ip route 0.0.0.0 0.0.0.0 80.1.1.100 250
```

Network Address Translation (NAT)

NAT и резервирование провайдеров

Два outside интерфейса

Если на маршрутизаторе Cisco созданы два правила для динамической трансляции, он выбирает правило в порядке создания. К сожалению, не учитывается то, через какой интерфейс маршрутизируется пакет.

Поэтому, когда на маршрутизаторе два outside интерфейса, правила трансляции необходимо настраивать с route-map

Таблица трансляций

При переключении между провайдерами, возникает проблема с подвисшими сессиями (как правило, TCP).

Для её решения используется EEM. EEM автоматически очищает таблицу трансляций, после каждого переключения.

NAT с двумя outside интерфейсами

```
interface GigabitEthernet0/0
  ip nat inside
!
interface GigabitEthernet0/1
  ip nat outside
!
interface GigabitEthernet0/2
  ip nat outside
!
ip access-list extended LAN
  permit ip 10.1.0.0 0.0.255.255 any
!
route-map ISP_1 permit 10
  match ip address LAN
  match interface GigabitEthernet0/1

route-map ISP_2 permit 10
  match ip address LAN
  match interface GigabitEthernet0/2
!
ip nat inside source route-map ISP_1 interface Gi0/1 overload
ip nat inside source route-map ISP_2 interface Gi0/2 overload
```


Embedded Event Manager (EEM)

Embedded Event Manager (EEM)

EEM это функционал встроенный в Cisco IOS, который позволяет создавать сценарии для автоматизации работы устройств.

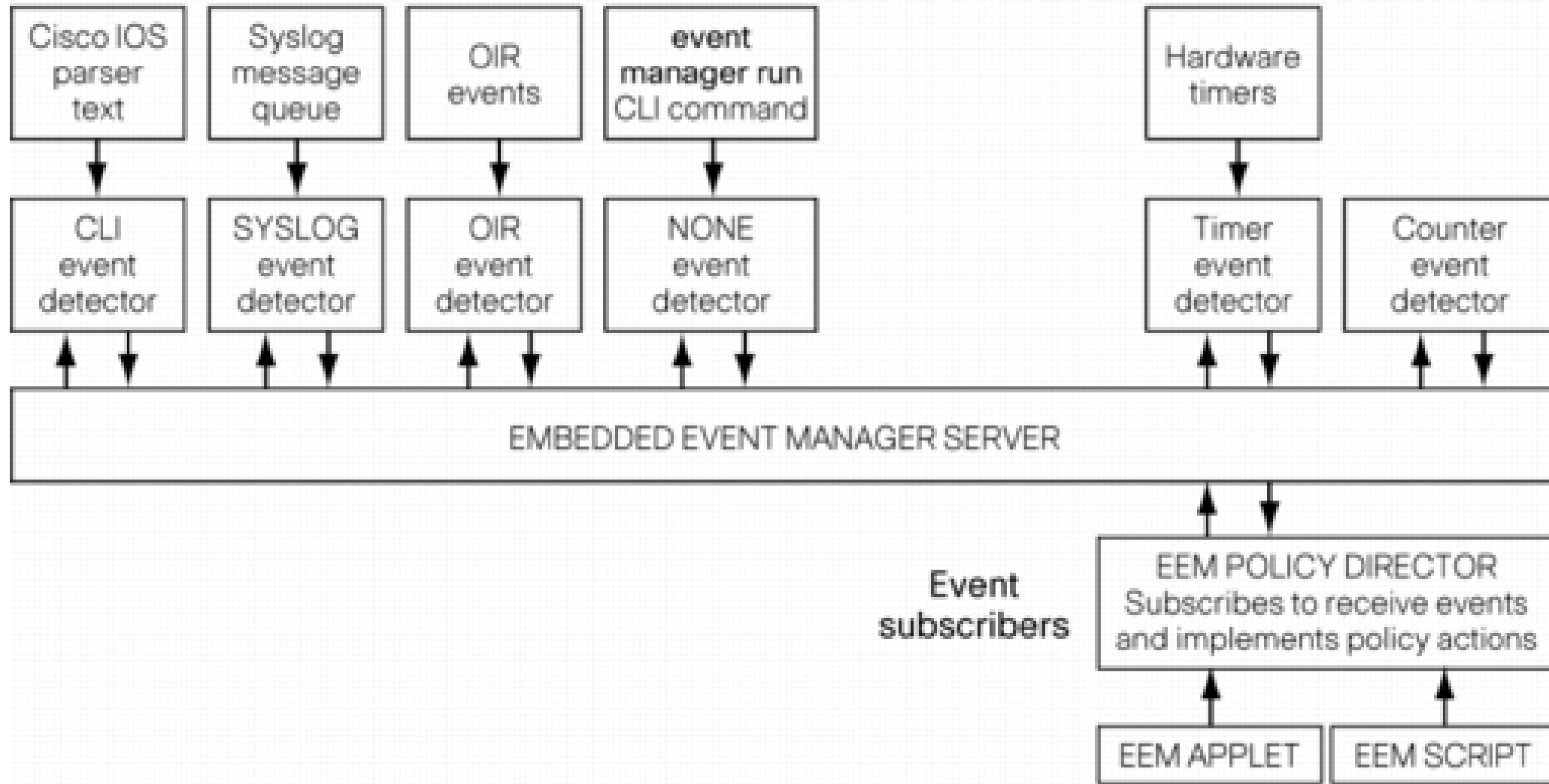
Причиной для выполнения сценария является событие.

Например, событием может быть изменение состояния track, запуск сценария вручную, выполнение команды и другие.

Сам сценарий может состоять из перечня команд, которые нужно выполнить; генерации syslog-сообщения и другие.

Embedded Event Manager (EEM)

Core event publishers



Пример правила

Создание правила:

```
router(config)#event manager applet INT_DOWN
```

Настройка события на которое ЕЕМ будет реагировать:

```
router(config-applet)# event syslog pattern "Interface  
GigabitEthernet0/0, changed state to down"
```

Настройка действий, которые будут выполнены, после того как произошло событие:

```
router(config-applet)# action 001 cli command "enable"  
router(config-applet)# action 002 cli command "configure term"  
router(config-applet)# action 003 cli command "interface g0/1"  
router(config-applet)# action 004 cli command "no shut"
```

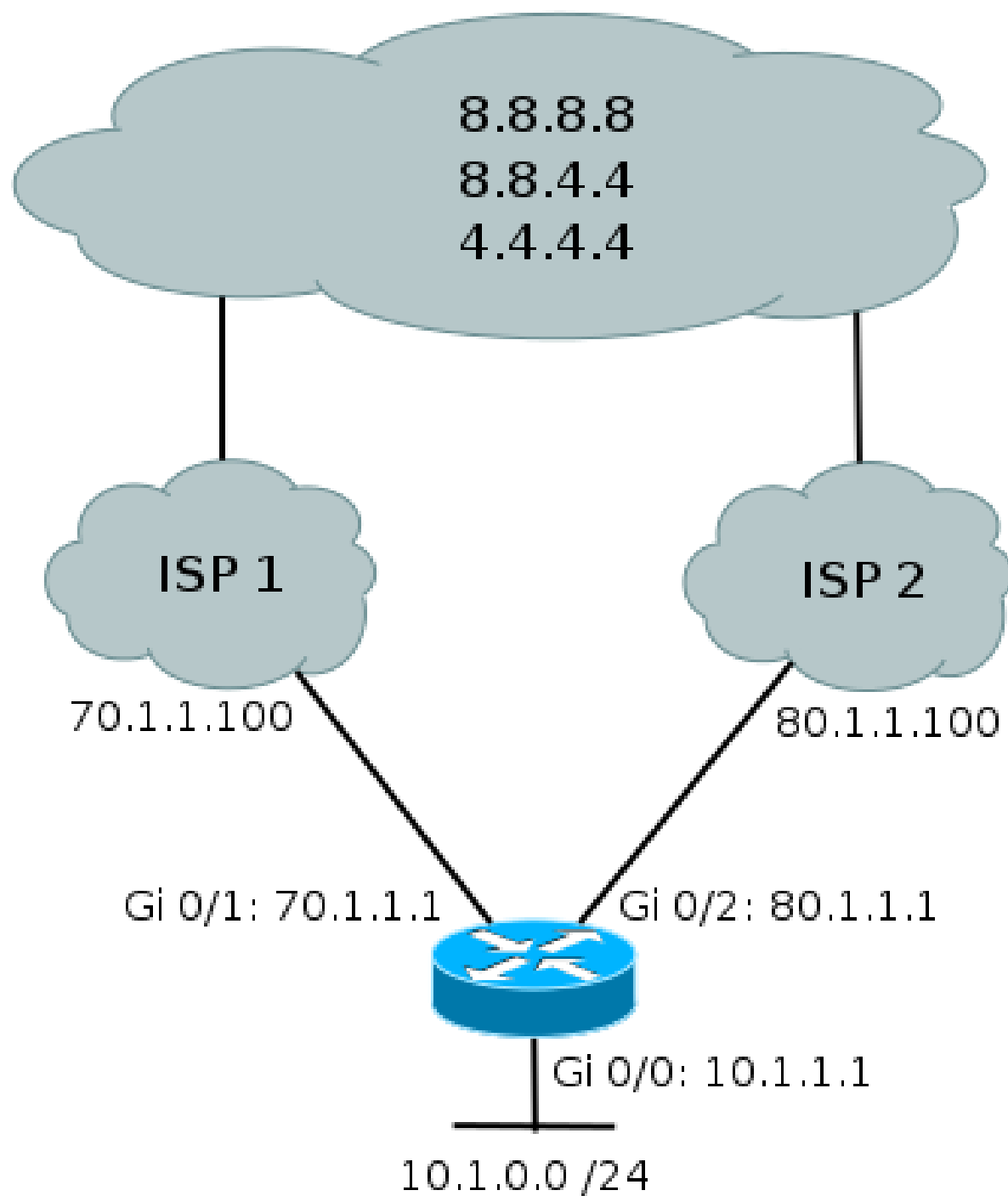
Настройка правил для автоматической очистки таблицы трансляций

```
event manager applet TRACK_ISP
  event track 1 state any
  action 001 cli command "enable"
  action 002 cli command "clear ip nat trans *"
  action 003 syslog msg "Track state is changed"
```

```
event manager applet ISP_1_UP
  event track 1 state up
  action 001 cli command "enable"
  action 002 cli command "clear ip nat trans *"
  action 003 syslog msg "ISP 1 is UP"
event manager applet ISP_1_DOWN
  event track 1 state down
  action 001 cli command "enable"
  action 002 cli command "clear ip nat trans *"
  action 003 syslog msg "ISP 1 is DOWN"
```

**Настройка резервирования каналов в сети
с одним пограничным маршрутизатором и
двумя каналами к разным провайдерам.
Без балансировки нагрузки**

Топология сети



Необходимые настройки

IP SLA	Настроить IP SLA тесты, которые будут мониторить несколько ресурсов.
Local PBR	Настроить политику PBR для тестов IP SLA. Политика будет отправлять пакеты, которые генерирует тест, на определенного провайдера
Track	Настроить track, который будет следить за соответствующим тестом IP SLA, а также суммарный track
Статическая маршрутизация	Настроить маршрут по умолчанию на основного провайдера и применить к нему суммарный трек. На резервного провайдера настроить маршрут по умолчанию со значением AD, большим чем 1
NAT	Настроить правила динамической трансляции, с использованием route-map
EEM	Настроить сценарий EEM, который будет автоматически очищать таблицу трансляции, после переключение провайдера

Настройка IP SLA тестов (icmp-echo)

```
ip sla 1
  icmp-echo 8.8.8.8 source-interface Gi0/1
  threshold 1000
  timeout 1500
  frequency 3
ip sla schedule 1 life forever start-time now
```

```
ip sla 2
  icmp-echo 8.8.4.4 source-interface Gi0/1
  threshold 1000
  timeout 1500
  frequency 3
ip sla schedule 2 life forever start-time now
```

```
ip sla 3
  icmp-echo 4.4.4.4 source-interface Gi0/1
  threshold 1000
  timeout 1500
  frequency 3
ip sla schedule 3 life forever start-time now
```

Нюансы настройки IP SLA

Мониторить лучше стабильные ресурсы.

В тесте обязательно надо указывать IP-адрес отправителя или интерфейс.

Параметры теста:

Threshold – устанавливает верхнее пороговое значение для измерения RTT (round-trip time)

Timeout – период времени, который IOS ожидает ответ на пакеты теста

Frequency – частота отправки тестовых пакетов

Проверка IP SLA

```
R1#sh ip sla summary
```

```
IPSLAs Latest Operation Summary
```

ID	Type	Destination	Stats (ms)	Return Code	Last Run
*1	icmp-echo	8.8.8.8	RTT=1	OK	1 second ago
*2	icmp-echo	8.8.4.4	RTT=1	OK	2 seconds ago
*3	icmp-echo	4.4.4.4	RTT=1	OK	1 second ago

```
R1#sh ip sla statistics 1
```

```
IPSLAs Latest Operation Statistics
```

```
IPSLA operation id: 1
```

```
Latest RTT: 1 milliseconds
```

```
Latest operation start time: 10:22:19 UTC Wed Feb 18 2015
```

```
Latest operation return code: OK
```

```
Number of successes: 741
```

```
Number of failures: 0
```

```
Operation time to live: Forever
```

Настройка Local PBR

Настройка Local PBR нужна для того, чтобы, при переключении провайдера, пакеты теста шли через основного провайдера.

```
ip access-list extended SLA_ACL
  permit icmp host 70.1.1.1 host 8.8.8.8
  permit icmp host 70.1.1.1 host 8.8.4.4
  permit icmp host 70.1.1.1 host 4.4.4.4
```

```
route-map PBR_SLA permit 10
  match ip address SLA_ACL
  set ip next-hop 70.1.1.100
```

```
ip local policy route-map PBR_SLA
```

Проверка Local PBR

R1#sh access-lists SLA_ACL

Extended IP access list SLA_ACL

10 permit icmp host 70.1.1.1 host 8.8.8.8 (17 matches)

20 permit icmp host 70.1.1.1 host 8.8.4.4 (16 matches)

30 permit icmp host 70.1.1.1 host 4.4.4.4 (17 matches)

R1#sh route-map PBR_SLA

route-map PBR_SLA, permit, sequence 10

Match clauses:

ip address (access-lists): SLA_ACL

Set clauses:

ip next-hop 70.1.1.100

Policy routing matches: 29 packets, 1856 bytes

R1#sh ip local policy

Local policy routing is enabled, using route map PBR_SLA

route-map PBR_SLA, permit, sequence 10

Match clauses:

ip address (access-lists): SLA_ACL

Set clauses:

ip next-hop 70.1.1.100

Policy routing matches: 199 packets, 12736 bytes

Настройка Track

Каждый track (10,20,30) отслеживает свой тест IP SLA.
Суммарный track 100 объединяет созданные track.
Настройка “boolean or” обозначает, что суммарный track будет в состоянии UP, если хотя бы один из track в состоянии UP.

```
track 10 ip sla 1 reachability
track 20 ip sla 2 reachability
track 30 ip sla 3 reachability
```

```
track 100 list boolean or
  object 10
  object 20
  object 30
  delay down 10 up 5
```

Нюансы настройки Track

При настройке связки IP SLA и Track, есть два варианта: state и reachability:

```
track 50 ip sla 5 state
track 50 ip sla 5 reachability
```

Отличия этих вариантов настройки в том, как они работают с кодом OverThreshold

State:

- Up — код OK

- Down — другие коды

Reachability:

- Up — код OK или код OverThreshold

- Down — другие коды

Нюансы настройки Track (продолжение)

Параметр “**delay**” в настройке track 100 нужен для того, чтобы track переходил в состояние DOWN с задержкой. Иначе, как только пропадет хотя бы один пакет ICMP, track перейдет в состояние DOWN.

Параметр delay настраивается в соответствии с частотой отправки ICMP-запросов.

В нашем примере, частота 3 секунды, а задержка на переход в состояние DOWN 10 секунд. То есть, track 100 перейдет в состояние DOWN только если все тесты перестали получать ответы. И не получили, как минимум 3 ответа.

Аналогично с переходом в состояние UP.

Проверка Track

R1#sh track

Track 10

IP SLA 1 reachability

Reachability is Up

3 changes, last change 4d20h

Latest operation return code: OK

Latest RTT (millisecs) 1

Tracked by:

Track-list 100

...

Track 100

List boolean or

Boolean OR is Up

4 changes, last change 4d20h

object 10 Up

object 20 Up

object 30 Up

Delay up 10 secs, down 5 secs

Tracked by:

Настройка статической маршрутизации

К маршруту по умолчанию, который ведет к основному провайдеру, должен быть применен суммарный track.

А у маршрута, который ведет к резервному провайдеру, значение AD должно быть увеличено.

```
ip route 0.0.0.0 0.0.0.0 70.1.1.100 track 100  
ip route 0.0.0.0 0.0.0.0 80.1.1.100 250
```

Проверка статической маршрутизации

R1#sh ip route track-table

```
ip route 0.0.0.0 0.0.0.0 70.1.1.100 track 100 state is [up]
```

R1#sh track 100

Track 100

List boolean or

Boolean OR is Up

4 changes, last change 4d20h

object 10 Up

object 20 Up

object 30 Up

Delay up 5 secs, down 5 secs

Tracked by:

STATIC-IP-ROUTING 0

Настройка NAT

```
interface GigabitEthernet0/0
 ip nat inside
!
interface GigabitEthernet0/1
 ip nat outside
!
interface GigabitEthernet0/2
 ip nat outside
!
ip access-list extended LAN
 permit ip 10.1.0.0 0.0.255.255 any
!
route-map ISP_1 permit 10
 match ip address LAN
 match interface GigabitEthernet0/1
!
route-map ISP_2 permit 10
 match ip address LAN
 match interface GigabitEthernet0/2
!
ip nat inside source route-map ISP_1 interface Gi0/1 overload
ip nat inside source route-map ISP_2 interface Gi0/2 overload
```

Проверка NAT

R1#sh ip nat statistics

```
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Peak translations: 92, occurred 5d20h ago
Outside interfaces:
  GigabitEthernet0/1, GigabitEthernet0/2
Inside interfaces:
  GigabitEthernet0/0
Hits: 822   Misses: 0
CEF Translated packets: 85, CEF Punted packets: 397
Expired translations: 142
Dynamic mappings:
-- Inside Source
[Id: 3] route-map ISP_1 interface GigabitEthernet0/1 refcount 0
[Id: 4] route-map ISP_2 interface GigabitEthernet0/2 refcount 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

R1#sh ip nat translations

Настройка EEM

Каждый сценарий EEM срабатывает на смену состояния суммарного track.

После обнаружения смены состояния, сценарий выполняет очистку таблицы трансляций и генерирует log-сообщение. Если эту очистку не выполнять, сессии TCP останутся в подвисшем состоянии.

```
event manager applet ISP_1_UP
  event track 100 state up
  action 001 cli command "enable"
  action 002 cli command "clear ip nat trans *"
  action 003 syslog msg "ISP 1 is UP"
```

```
event manager applet ISP_1_DOWN
  event track 100 state down
  action 001 cli command "enable"
  action 002 cli command "clear ip nat trans *"
  action 003 syslog msg "ISP 1 is DOWN"
```

Проверка EEM

R1#sh event manager policy registered

No.	Class	Type	Event	Trap	Time	Registered	Name
1	applet	user	track	Off	Fri Feb 13 14:09:29 2015	ISP_1_DOWN	
track 200 state down							
maxrun 20.000							
action 001 cli command "enable"							
action 002 cli command "clear ip nat translation *"							
action 003 syslog msg "ISP 1 is DOWN"							
2	applet	user	track	Off	Fri Feb 13 14:11:08 2015	ISP_1_UP	
track 200 state up							
maxrun 20.000							
action 001 cli command "enable"							
action 002 cli command "clear ip nat translation *"							
action 003 syslog msg "ISP 1 is UP"							

Проверка EEM

```
router1#sh track 100
```

```
Track 100
```

```
List boolean or
```

```
Boolean OR is Up
```

```
4 changes, last change 4d20h
```

```
object 10 Up
```

```
object 20 Up
```

```
object 30 Up
```

```
Delay up 5 secs, down 5 secs
```

```
Tracked by:
```

```
STATIC-IP-ROUTING 0
```

```
EEM applet ISP_1_DOWN
```

```
EEM applet ISP_1_DOWN
```


Резервирование Интернет-каналов без использования BGP.

**Автор курса: Наташа Самойленко
nataliya.samoylenko@gmail.com**